Software Release Note

AlliedWare Plus Version 5.3.4-0.1

For SwitchBlade x908, x900 Series, and x600 Series Switches

Contents

Introduction....1
Acknowledgements....2
New Features and Enhancements....3
Changes in this Version....6
Installing this Software Version....23
Installing the GUI....24
Errata to the Software Reference....26
icmp-redirect (x600)....26
sflow agent (address)....27
GUI Errata....28

Introduction

This release note describes the new features and enhancements in AlliedWare Plus software version 5.3.4 since version 5.3.3. For more information, see the Software Reference for your switch. Software file details for this version are listed in Table 1 below. There is a new GUI file for this version; the GUI file listed in the table below for use with software version 5.3.4 is not the same as for software version 5.3.3.

Table 1: Switch models and software file names

Models	Series	Software File	Date	GUI File[1]
x600-24Ts, x600-24Ts/XP, x600-48Ts, x600-48Ts/XP	x600	r6-5.3.4-0.1.rel	4 July 2010	gui_534_06.jar
x600-24Ts-POE	x600	r6-5.3.4-0.1.rel	4 July 2010	gui_534_06.jar
x900-12XT/S, x900-24	x900	r1-5.3.4-0.1.rel	4 July 2010	gui_534_06.jar
SwitchBlade x908	SwitchBlade	r1-5.3.4-0.1.rel	4 July 2010	gui_534_06.jar

1. GUI updates: This GUI version supports configuring PoE on the x600-24Ts-POE. Support for the XEM-2XP module for x908/x900 series switches has been added.

Caution: Using a software version file for the wrong switch model may cause unpredictable results, including disruption to the network. Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesis, Inc. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesis, Inc. can not accept any type of liability for errors in, or omissions arising from, the use of this information.

Acknowledgements

This product includes software developed by the University of California, Berkeley and its contributors.
Copyright ©1982, 1986, 1990, 1991, 1993 The Regents of the University of California.
All rights reserved.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).
Copyright ©1998-2008 The OpenSSL Project. All rights reserved.

This product includes software licensed under the GNU General Public License available from:
http://www.gnu.org/licenses/gpl2.html

Source code for all GPL licensed software in this product can be obtained from the Allied Telesis GPL Code Download Center at:
http://www.alliedtelesis.com/support/default.aspx

Allied Telesis is committed to meeting the requirements of the open source licenses including the GNU General Public License (GPL) and will make all required source code available.

If you would like a copy of the GPL source code contained in Allied Telesis products, please send us a request by registered mail including a check for US$15 to cover production and shipping costs and a CD with the GPL code will be mailed to you.

GPL Code Request
Allied Telesis Labs (Ltd)
PO Box 8011
Christchurch.
New Zealand

©2010 Allied Telesis, Inc. All rights reserved.

This documentation is subject to change without notice. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's internal use without the written permission of Allied Telesis, Inc.

Allied Telesis, AlliedWare Plus, EPSRing, SwitchBlade, and VCStack are trademarks or registered trademarks in the United States and elsewhere of Allied Telesis, Inc. Adobe, Acrobat, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Additional brands, names and products mentioned herein may be trademarks of their respective companies.

New Features and Enhancements

This software version includes the following main new features. For a list of all new and enhanced features and commands, see "Changes in this Version" on page 6. For more information about all features on the switch, see the Software Reference for your switch. Unless otherwise stated, all new features and enhancements are available on all switch models running this version of AlliedWare Plus.

VCStack Fast Failover

Virtual Chassis Stacking (VCStack) delivers resiliency and scalability to networks, simplifying management while increasing performance. VCStack Fast Failover further enhances this advanced solution by providing absolutely minimal network downtime in the event of a problem, by reducing traffic interruption across the stack following master failover.

The time taken for VCStack to recover and forward traffic following a stack failure has been dramatically reduced. With this feature VCStack will in most cases resume and traffic will flow within six seconds of master failover. Fast Failover reduces traffic interruption across the stack following master failover. The time for the tested solution for VCStack failover to run has reduced from 14 seconds to under 1 second with the enhancements to VCStack in this release.

XEM-2XP Support (x908/x900 series)

This release supports the XEM-2XP module with 10G XFP ports for resilient 10G EPSRring.

sFlow Agent

sFlow® is an industry standard technology for monitoring high speed switched networks. It provides the ability to monitor traffic in data networks containing switches and routers. It gives complete visibility into the use of networks enabling performance optimization, accounting/ billing for usage, and defence against security threats. Sampled packets sent to a collector ensure it has a real-time view of network traffic.

sFlow® can be used to identify network bottlenecks and high bandwidth consumers. sFlow lowers the cost of network resources when Network Administrators can optimize networks using existing equipment and improving network design, instead of purchasing new equipment.

DHCP Snooping

DHCP servers allocate IP addresses to clients, and the switch keeps a record of addresses issued on each port. DHCP Snooping can be used to increase network security and traceability by filtering traffic according to valid DHCP leases. DHCP snooping on the switch supports traffic filtering, DHCP Option 82, ARP security, and MAC address verification.

DHPCP Snooping is used to keep a record of which IP address are currently allocated to hosts downstream of the ports on the switch. DHCP Snooping prevents attackers from spoofing an IP address because the switch is aware of authorized IP addresses to drop any untrusted hosts.

DHCP Lease Deletion

On dynamically allocated bindings the new command for this feature clears either a specific lease binding, or the lease bindings specified by the new command.

ARP Logging

You can enable your device to log static and dynamic ARP entries, and you can select either default hexadecimal notation (HHHH.HHHH.HHHH) or standard IEEEE format hexadecimal notation (HH-HH-HH-HH-HH-HH) for the MAC addresses displayed in the ARP log output.

ACL Sequence Number Support

To help you manage ACLs you can apply sequence numbers to filters. This allows you to remove filters from named and numbered ACLs without having to reconfigure an ACL. The ability to add sequence numbers to filters simplifies updates through the ability to position a filter within an ACL. When you add a new filter, you can specify a sequence number to position the filter in the ACL. You can remove a filter in an ACL by specifying a sequence number too.

Triggers Enhancements (VCStack)

This feature introduces trigger command enhancements (configured for VCStack) to enable simpler and more stable VCStack configurations to be created. The user can select a pre-configured trigger that will activate on a stack member if it becomes the disabled master. This feature deprecates the VCStack fallback config feature available in previous releases.

Diagnostic Monitoring (Background PCS Ping) (x908/x900 series)

PCS (Physical Coding Sublayer) ping is an automatically enabled hardware feature used to continuously check the link status between an expansion module (XEM) and the switch. This feature checks XEM modules that are installed in an x908/x900 switch. It also checks the x908 switch without a XEM module installed, and output a log message if the x908 is found faulty.

A new command is available to disable or configure the background PCS ping monitoring feature to output a log message or to power off a XEM when background PCS ping check fails.

Authentication Enhancements

The authentication enhancements introduced in this release fall into three areas: improvements to Web-authentication, increased flexibility in the operation of the Guest VLAN, and introduction of the auth-fail VLAN to make the authentication features easier to configure and more usable.

Web-authentication Enhancements

These enhancements ensure that the client PC user is presented with the Web-authentication login page as soon as they start web browsing to any address, irrespective of the IP configuration on their PC.

Guest VLAN Enhancements

These enhancements ensure that the client PC user is presented with the Web-authentication login page as soon as they start web browsing to any address, irrespective of the IP configuration on their PC.

Failed authentication Enhancements

The auth-fail VLAN feature allows the Network Administrator to separate the supplicants that attempted authentication, but failed, from the supplicants that did not attempt authentication.

GUI Enhancements

This GUI version now supports the x600-24Ts-POE, plus stacked and standalone x600 series, x900 series, and x908 SwitchBlade switches. A PoE GUI tab is shown for the x600-24Ts-POE. Support for the XEM-2XP has been added in the GUI for x908/x900 series switches.
The PoE feature on x600-24Ts-POE can now be configured using this version of the GUI.

100 LAG License (x600 series only)

With this feature license you can create a total of 100 channel groups, with a combination of up to 96 static channel groups and up to 32 dynamic channel groups. A total of 100 channel groups, comprised of static and dynamic channel groups, is the supported limit with this license.

100 PIM License (x900 series only)

With this feature license you can create a total of 100 PIM interfaces (using either PIM-SM or PIM-DM). The supported limit with this license is a total of 100 PIM interfaces, which can be a combination of PIM-SM and PIM-DM interfaces (100 PIM interfaces of PIM-SM and PIM-DM).

Strong Passwords

This feature enables the implementation of a high security password policy that can control password definition, password expiry date, and account lockout options upon login failure.

This feature introduces new commands that use the password security rules to specify a password lifetime, either to force a user to change an expired password at the next login, or to specify that a user is not allowed to login with an expired password, set the number of previous passwords unable to be reused, and specify password minimum length and categories.

BGP Authentication

This feature enables the receipt of selected routing information, enhancing the security of network traffic. When BGP authentication is enabled on a peer, the peer verifies the packet it receives by exchanging a password that is configured on both sending and receiving peers.

SDHC Support

This release supports the use of both SD cards and SDHC cards to upload and backup files.

RIP, RIPng, OSPF, BGP Graceful Reset and Graceful Restart

The graceful restart feature for RIP, RIPng, OSPF, and BGP session reset is used so that any changes in network configuration do not affect packet forwarding. Using RIP, RIPng, OSPF, and BGP graceful restart and graceful reset, the switch can continue to process and forward packets even after failover without traffic loss.

Changes in this Version

Table 2 below lists all new and modified features and commands in this version.

If your existing configurations include commands modified or deleted in this version (see the Status column), check whether you need to modify these configurations. For full command descriptions, see Software Reference for your switch.

Table 2: New and modified features and commands

Feature/ Command/ MIB	Type	Status	x600	x908/x900	Software Reference Chapter	Description
Strong Passwords						
How to Set Strong Passwords	Feature	New	Y	Y	Getting Started	Use the password security rules to specify a password lifetime, force a user to change an expired password at the next login, specify that a user is not allowed to login with an expired password, set the number of previous passwords unable to be reused, and specify password minimum length and categories.
security-password history	Command	New	Y	Y	User Access Commands	This command specifies the number of previous passwords that are unable to be reused.
security-password forced-change	Command	New	Y	Y	User Access Commands	This command specifies whether or not a user is forced to change an expired password at the next login.
security-password lifetime	Command	New	Y	Y	User Access Commands	This command enables password expiry by specifying a password lifetime in days.
security-password minimum-categories	Command	New	Y	Y	User Access Commands	This command configures the minimum number of categories that the password must satisfy to be considered valid.
security-password minimum-length	Command	New	Y	Y	User Access Commands	This command configures the minimum allowable password length.
security-password reject-expired-pwd	Command	New	Y	Y	User Access Commands	This command specifies whether or not a user is allowed to login with an expired password.
security-password warning	Command	New	Y	Y	User Access Commands	This command specifies the number of days before the password expires that the user will receive a warning message specifying the remaining lifetime of the password.
show security-password configuration	Command	New	Y	Y	User Access Commands	This command displays the configuration settings for the various security password rules.
show security-password user	Command	New	Y	Y	User Access Commands	This command displays user account and password information for all users
show running-config security-password	Command	New	Y	Y	File Management Commands	This command displays the configuration settings for the various security-password rules.
boot system (file-path|URL)	Command	New	Y	Y	System Configuration and Monitoring Commands	This command specifies the release file that will load during the next boot cycle. The specified file must exist and be stored in the root directory of the flash filesystem.

Table 2: New and modified features and commands

Feature/ Command/ MIB	Type	Status	x600	x600/806x	Software Reference Chapter	Description
Diagnostic Monitoring (Backgroup PCS Ping)						
diagnostic monitor pcsping	Command	New	N	Y	System Configuration and Monitoring Commands	Use this command to disable or configure the background PCS (Physical Coding Sublayer) ping monitoring feature to either output a log message or to power off a XEM when a background PCS ping check fails. The background PCS ping feature is enabled by default to output log messages.
show diagnostic monitor pcsping	Command	New	N	Y	System Configuration and Monitoring Commands	Use this command show the status of the background PCS (Physical Coding Sublayer) ping feature used to the check the link status between a XEM and the switch.
Miscellaneous Feature Updates						
show debugging	Command	New	Y	Y	System Configuration and Monitoring Commands	This command displays information for all debugging options.
speed (async)	Command	New	Y	Y	System Configuration and Monitoring Commands	This command changes the console speed from the switch.
log-rate-limit nsm	Command	New	Y	Y	Logging Commands	This command limits the number of log messages generated by the switch. The log rate limiting feature resolves the issue of the switch memory becoming overloaded, which may cause the switch to shutdown, when a packet storm occurs, because of a network loop generating too many log messages too frequently for memory.
mru	Command	Modified	Y	N	Interface Commands	The MRU (Maximum Receive Unit) size can be set using this command for a switch port (MTU can only be set on a VLAN interface). The negated form of this command restores the default MRU size of 1500 bytes for a switch port.
mtu	Command	Modified	Y	Y	Interface Commands	The MTU (Maximum Transmission Unit) size for VLANs specified by this command has changed from <64-9208> bytes to <68-1500> bytes. The negated form of this command will restore the default MTU size of 1500 bytes for VLANs.
show interface brief	Command	Modified	Y	Y	Interface Commands	This command displays brief interface, configuration, and status information, including provisioning information.
debug loopprot	Command	New	Y	Y	Switching Commands	This command enables Loop Protection debugging.

Table 2: New and modified features and commands

Feature/ Command/ MIB	Type	Status	x600	x900/x908	Software Reference Chapter	Description
debug platform packet	Command	Modified	Y	Y	Switching Commands	The sflow parameter option has been added to the debug platform packet command to display only sFlow packets when enabled. The vlan parameter option has also been added to the debug platform packet command to limit debug to a single VLAN ID specified when enabled.
platform enhancedmode	Command	Modified	N	Y	Switching Commands	This command rearranges memory in the silicon so that it can store a greater than usual number of QoS traffic class counters, QoS Policers, or nexthop routes. For the enhanced mode to take effect, you must restart the device after entering this command. The qospolicers parameter has been added.
platform portstorm	Command	Modified	N	Y	Switching Commands	This command performs a port storm on the system. This test generates a high packet load on switch ports, exercising the packet data path and front-panel ports.
platform prbs	Command	Modified	N	Y	Switching Commands	This command performs a PRBS (Pseudo-Random Bit Stream) test on the switch.You can now specify whether to test either the internal fabric links or the stacking fabric links (x908 only), or both.
platform routingratio	Command	Modified	N	Y	Switching Commands	This command changes the amount of memory allocated to IPv4 routing tables relative to IPv6 routing tables. The default routing memory ratio is now set to ipv4andipv6 allowing both IPv4 and IPv6 to run concurrently.
platform vlan-stacking-tpid	Command	Modified	Y	Y	Switching Commands	The no platform vlan-stacking-tpid command has been added to revert to the default TPID (Tag Protocol Identifier) value of 0x8100.
show debugging loopprot	Command	New	Y	Y	Switching Commands	This command shows Loop Protection debugging information.
show debugging platform packet	Command	New	Y	Y	Switching Commands	This command shows platform to CPU level packet debugging information.
show platform full debug	Command	New	Y	Y	Switching Commands	This command displays low-level system information and diagnostics.
show platform portstorm	Command	Modified	N	Y	Switching Commands	This command displays the result of a previously run port storm test on the switch.
Provisioning						
show provisioning (xem-bay)	Command	New	N	Y	Switching Commands	This command shows the provisioning status of all installed or provisioned hardware.
switch bay provision	Command	New	N	Y	Switching Commands	This command enables you to pre configure a specific empty bay within a switch ready for inserting a particular XEM type. To run this command, the bay position must be vacant and the selected XEM type must be one that is currently supported.

Table 2: New and modified features and commands

Feature/ Command/ MIB	Type	Status	x600	x900/x908	Software Reference Chapter	Description
100 LAG License (x600 only)						
channel-group mode	Command	Modified	Y	N	Link Aggregation Commands	With this command you add a switch port to a dynamic channel group specified by the channel group number. You can now create 32 channel groups with a base license, consisting of a combination of static and dynamic channel groups. With a feature license you can create up to 100 channel groups, consisting of up to 32 dynamic channel groups and up to 96 static channel groups to total up to 100 static channel groups and dynamic channel groups combined.
static-channel-group	Command	Modified	Y	N	Link Aggregation Commands	With this command you can create a static channel group, or add a member port to an already existing static channel group. You can now create 32 channel groups with a base license, consisting of a combination of static and dynamic channel groups. With a feature license you can create up to 100 channel groups, consisting of up to 96 static channel groups and up to of 32 dynamic channel groups to total up to 100 static channel groups and dynamic channel groups combined.
ARP Logging						
ARP Logging	Feature	New	Y	Y	Internet Protocol (IP) Addressing and Protocols	You can enable your device to log static and dynamic ARP entries, and you can select either default hexadecimal notation (HHHH.HHHH.HHHH) or standard IEEE format hexadecimal notation (HH-HH-HH-HH-HH-HH) for the MAC addresses displayed in the ARP log output.
arp log	Command	New	Y	Y	IP Addressing and Protocol Commands	This command enables and disables the logging of dynamic and static ARP entries in the ARP cache. This command can display the MAC addresses in the ARP log either using the default hexadecimal notation (HHHH.HHHH.HHHH), or using the standard IEEE format notation (HH-HH-HH-HH-HH-HH).
RIP						
cisco-metric-behavior (RIP)	Command	New	Y	Y	RIP Commands	Use this command to enable or disable the RIP routing metric update to conform to Cisco's implementation. The Cisco implementation sets the metric of redistributed connected and static RIP routes to 0 by default. AlliedWare Plus sets this metric to 1 by default when using the default-metric command.

Table 2: New and modified features and commands

Feature/ Command/ MIB	Type	Status	x600	x600/x908x	Software Reference Chapter	Description
RIPng						
cisco-metric-behavior (RIPng)	Command	New	Y	Y	RIPng Commands	Use this command to enable or disable the RIPng routing metric update to conform to Cisco's implementation. The Cisco implementation sets the metric of redistributed connected and static RIPng routes to 0 by default. AlliedWare Plus sets this metric to 1 by default when using the default-metric command.
OSPF						
enable db-summary-opt	Command	New	Y	Y	OSPF Commands	This command enables OSPF database summary list optimization.
network area	Command	Modified	Y	Y	OSPF Commands	Use this command to enable OSPF routing with a specified Area ID on interfaces with IP addresses that match the specified network address.
passive-interface (OSPF)	Command	Modified	Y	Y	OSPF Commands	Use this command to suppress the sending of Hello packets on all interfaces, or on a specified interface. If you use the passive-interface command without the optional parameters then all interfaces are put into passive mode.
timers spf exp	Command	New	Y	Y	OSPF Commands	Use this command to adjust route calculation timers using exponential back-off delays.
BGP						
BGP Authentication	Feature	New	Y	Y	BGP Configuration	BGP authentication allows users to receive selected routing information, enhancing security of their network traffic. When BGP authentication is enabled on a peer, the peer verifies routing packet it receives by exchanging a password that is configured on both the sending and the receiving peers.
Configuring BGP Graceful Reset	Feature	New	Y	Y	BGP Configuration	The graceful restart feature for BGP session reset is used so that any changes in network configuration do not affect packet forwarding. The graceful restart feature invokes graceful restart only when a configuration change forces a peer reset.
Configuring BGP Graceful Restart	Feature	New	Y	Y	BGP Configuration	Using BGP graceful restart, the data forwarding plane of the device can continue to process and forward packets even if the control plane, which is responsible for determining best paths, fails
bgp bestpath med remove-recv-med	Command	New	Y	Y	BGP Commands	This command removes the Multi Exit Discriminator (MED) attribute from the update messages received by the BGP speaker from its peers.
bgp bestpath med remove-send-med	Command	New	Y	Y	BGP Commands	This command removes the Multi Exit Discriminator (MED) attribute from the update messages sent by the BGP speaker from its peers.

Table 2: New and modified features and commands

Feature/ Command/ MIB	Type	Status	x600	x900/x908	Software Reference Chapter	Description
bgp graceful-restart graceful-reset	Command	New	Y	Y	BGP Commands	This command enables BGP graceful-restart when a configuration change forces a peer restart.
bgp multiple-instance	Command	Modified	Y	Y	BGP Commands	This command enables the BGP multiple instance support. You now have the option to activate the same peer in multiple BGP views.
bgp nexthop-trigger-count	Command	New	Y	Y	BGP Commands	This command configures the display of BGP nexthop-tracking status.
bgp nexthop-trigger delay	Command	New	Y	Y	BGP Commands	This command sets the delay interval for nexthop address tracking.
bgp nexthop-trigger enable	Command	New	Y	Y	BGP Commands	This command enables nexthop address tracking.
neighbor connection-retry-time	Command	New	Y	Y	BGP Commands	This command sets the connection retry time for a specific BGP neighbor.
neighbor disallow-infinite-holdtime	Command	New	Y	Y	BGP Commands	Use this command to disallow the configuration of infinite holdtime.
neighbor password	Command	New	Y	Y	BGP Commands	Use this command to enable MD5 authentication on a TCP connection between BGP neighbors.
show bgp nexthop-tracking	Command	New	Y	Y	BGP Commands	This command displays BGP nexthop-tracking status.
show bgp nexthop-tree-details	Command	New	Y	Y	BGP Commands	This command displays BGP nexthop-tree-details.
show ip bgp neighbors connection-retrytime	Command	New	Y	Y	BGP Commands	This command displays the configured connection-retrytime value of the peer at the session establishment time with the neighbor.
show ip bgp neighbors hold-time	Command	New	Y	Y	BGP Commands	This command displays the configured holdtime value of the peer at the session establishment time with the neighbor.
show ip bgp neighbors keepalive	Command	New	Y	Y	BGP Commands	This command displays the number of keepalive messages sent to the neighbor from the peer throughout the session.
show ip bgp neighbors keepalive-interval	Command	New	Y	Y	BGP Commands	This command displays the configured keepalive-interval value of the peer at the session establishment time with the neighbor.
show ip bgp neighbors notification	Command	New	Y	Y	BGP Commands	This command displays the number of notification messages sent to the neighbor from the peer throughout the session.
show ip bgp neighbors open	Command	New	Y	Y	BGP Commands	This command displays the number of open messages sent to the neighbor from the peer throughout the session.
show ip bgp neighbors rcvd-msgs	Command	New	Y	Y	BGP Commands	This command displays the number of messages received by the neighbor from the peer throughout the session.

Table 2: New and modified features and commands

Feature/ Command/ MIB	Type	Status	x600	x900/x908	Software Reference Chapter	Description
show ip bgp neighbors sent-msgs	Command	New	Y	Y	BGP Commands	This command displays the number of messages sent to the neighbor from the peer throughout the session.
show ip bgp neighbors update	Command	New	Y	Y	BGP Commands	This command displays the number of update messages sent to the neighbor from the peer throughout the session.
timers (BGP)	Command	Modified	Y	Y	BGP Commands	This command sets the BGP keepalive timer and holdtime timer values. The default keepalive value has changed from 60 to 30 seconds and the default holdtime value has changed from 180 to 90 seconds.
PIM						
show ip pim sparse-mode interface	Command	Modified	N	Y	PIM-SM Commands	The output displayed by this command has changed. With the base license, the maximum number of PIM-SM interfaces that can be configured is 31. With a feature license a maximum of 100 interfaces are available. The show output will display the number of interfaces that can be configured in the “maximum allowed” field.
show ip pim dense-mode interface	Command	Modified	N	Y	PIM-DM Commands	The output displayed by this command has changed. With the base license, the maximum number of PIM-SM interfaces that can be configured is 32. With a feature license a maximum of 100 interfaces are available. The show output will display the number of interfaces that can be configured in the “maximum allowed” field.
ACL Sequence Number Support						
ACL Sequence Number Support	Feature	New	Y	Y	Access Control Lists Introduction	To help you manage ACLs you can apply sequence numbers to filters. This allows you to remove filters from named and numbered ACLs without having to reconfigure an ACL. The ability to add sequence numbers to filters simplifies updates through the ability to position a filter within an ACL. When you add a new filter, you can specify a sequence number to position the filter in the ACL and you can also remove a current filter in an ACL by specifying a sequence number.
access-group	Command	New	Y	Y	IPv4 Access Control List (ACL) Commands	This new command replaces the existing ip access group and mac access group commands. This command adds (or removes) a hardware-based numbered or named access-list to a switch port interface. This command works in both Global Configuration and Interface Configuration modes to apply hardware access-lists to all switch port interfaces or selected switch port interfaces respectively.

Table 2: New and modified features and commands

Feature/ Command/ MIB	Type	Status	x600	x900/x908	Software Reference Chapter	Description
access-list extended (named)	Command	Modified	Y	Y	IPv4 Access Control List (ACL) Commands	This command has been modified. This command configures an extended named access-list that permits or denies packets from specific source and destination IP addresses. You can either create an extended named ACL together with an ACL filter entry in the Global Configuration mode, or you can use the IPv4 Extended ACL Configuration mode for sequenced ACL filter entry.
access-list (extended numbered)	Command	Modified	Y	Y	IPv4 Access Control List (ACL) Commands	This command has been modified. This command configures an extended numbered access-list that permits or denies packets from specific source and destination IP addresses. You can either create an extended numbered ACL together with an ACL filter entry in the Global Configuration mode, or you can use the IPv4 Extended ACL Configuration mode for sequenced ACL filter entry.
access-list extended ICMP filter	Command	New	Y	Y	IPv4 Access Control List (ACL) Commands	Use this ACL filter to add a new ICMP filter entry to the current extended access-list. If the sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.
access-list extended IP filter	Command	New	Y	Y	IPv4 Access Control List (ACL) Commands	Use this ACL filter to add a new IP filter entry to the current extended access-list. If the sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.
access-list extended IP protocol filter	Command	New	Y	Y	IPv4 Access Control List (ACL) Commands	Use this ACL filter to add a new IP protocol type filter entry to the current extended access-list. If the sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.
access-list extended TCP UDP filter	Command	New	Y	Y	IPv4 Access Control List (ACL) Commands	Use this ACL filter to add a new TCP or UDP filter entry to the current extended access-list. If the sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.
access-list hardware (named)	Command	New	Y	Y	IPv4 Access Control List (ACL) Commands	This command creates a named hardware access-list that can be applied to a switch port interface. ACL filters for a named hardware ACL are created in the IPv4 Hardware ACL Configuration mode. The no variant of this command removes the specified named hardware ACL.

Table 2: New and modified features and commands

Feature/ Command/ MIB	Type	Status	x600	x900/x908	Software Reference Chapter	Description
access-list hardware ICMP filter	Command	New	Y	Y	IPv4 Access Control List (ACL) Commands	Use this ACL filter to add a new ICMP filter entry to the current hardware access-list. If a sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.
access-list hardware IP protocol filter	Command	New	Y	Y	IPv4 Access Control List (ACL) Commands	Use this ACL filter to add an IP protocol type filter entry to the current hardware access-list. If a sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.
access-list hardware MAC filter	Command	New	Y	Y	IPv4 Access Control List (ACL) Commands	Use this ACL filter to add a MAC filter entry to the current hardware access-list. If a sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.
access-list hardware TCP UDP filter	Command	New	Y	Y	IPv4 Access Control List (ACL) Commands	Use this ACL filter to add a TCP or UDP filter entry to the current hardware access-list. The filter will match on any TCP or UDP type packet that has the specified source and destination IP addresses. The parameter any may be specified if an address does not matter. If a sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.
access-list standard (named)	Command	Modified	Y	Y	IPv4 Access Control List (ACL) Commands	This command has been modified. This command configures a standard named access-list that permits or denies packets from a specific source IP address. You can either create a standard named ACL together with an ACL filter entry in the Global Configuration mode, or you can use the IPv4 Standard ACL Configuration mode for sequenced ACL filter entry.
access-list (standard numbered)	Command	Modified	Y	Y	IPv4 Access Control List (ACL) Commands	This command has been modified. This command configures a standard numbered access-list that permits or denies packets from a specific source IP address. You can either create a standard numbered ACL together with an ACL filter entry in the Global Configuration mode, or you can use the IPv4 Standard ACL Configuration mode for sequenced ACL filter entry.
access-list standard (named) filter	Command	New	Y	Y	IPv4 Access Control List (ACL) Commands	This ACL filter adds a source IP address filter entry to a current standard access-list. If the sequence number is specified, the new filter entry will be inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.

Table 2: New and modified features and commands

Feature/ Command/ MIB	Type	Status	x600	x900/x908	Software Reference Chapter	Description
access-list (standard numbered) filter	Command	New	Y	Y	IPv4 Access Control List (ACL) Commands	This ACL filter adds a source IP address filter entry to a current standard numbered access-list. If a sequence number is specified, the new filter entry is inserted at the specified location. Otherwise, the new filter entry is added at the end of the access-list.
ipv6 access-list extended (named)	Command	Modified	Y	Y	IPv6 Access Control List (ACL) Commands	Use this command when configuring an IPv6 extended access-list for filtering frames that permit or deny IP, ICMP, TCP, UDP packets or ICMP packets with a specific value based on the source or destination. The no variant of this command removes a specified IPv6 extended access-list.
ipv6 access-list extended IP protocol filter	Command	New	Y	Y	IPv6 Access Control List (ACL) Commands	Use this ACL filter to add a filter entry for an IPv6 source and destination address and prefix, with or without an IP protocol specified, to the current extended IPv6 access-list. If a sequence number is specified, the new entry is inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.
ipv6 access-list extended TCP UDP filter	Command	New	Y	Y	IPv6 Access Control List (ACL) Commands	Use this ACL filter to add a filter entry for an IPv6 source and destination address and prefix, with a TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) source and destination port specified, to the current extended IPv6 access-list. If a sequence number is specified, the new entry is inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.
ipv6 access-list (named)	Command	Modified	Y	Y	IPv6 Access Control List (ACL) Commands	Use this command to either create a new IPv6 hardware access-list, or to select an existing IPv6 hardware access-list in order to apply a filter entry to it. Use the no variant of this command to delete an existing IPv6 hardware access-list.
ipv6 access-list named ICMP filter	Command	Modified	Y	Y	IPv6 Access Control List (ACL) Commands	Use this ACL filter to add a filter entry for an IPv6 source and destination address and prefix, for ICMP (Internet Control Message Protocol) packets, to the current named IPv6 access-list. If a sequence number is specified, the new entry is inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.
ipv6 access-list named IPv6 protocol filter	Command	Modified	Y	Y	IPv6 Access Control List (ACL) Commands	Use this ACL filter to add a filter entry for an IPv6 source and destination address and prefix, with an IP protocol type specified, to the current named IPv6 access-list. If a sequence number is specified, the new entry is inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.

Table 2: New and modified features and commands

Feature/ Command/ MIB	Type	Status	x600	x900/x908	Software Reference Chapter	Description
ipv6 access-list named TCP UDP filter	Command	Modified	Y	Y	IPv6 Access Control List (ACL) Commands	Use this ACL filter to add a filter entry for an IPv6 source and destination address and prefix, with TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) source and destination ports specified, to the current named IPv6 access-list. If a sequence number is specified, the new entry is inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.
ipv6 access-list standard (named)	Command	Modified	Y	Y	IPv6 Access Control List (ACL) Commands	This command configures an IPv6 standard access-list for filtering frames that permit or deny IPv6 packets from a specific source IPv6 address. The no variant of this command removes a specified IPv6 standard access-list.
ipv6 access-list standard IPv6 filter	Command	New	Y	Y	IPv6 Access Control List (ACL) Commands	Use this ACL filter to add a filter entry for an IPv6 source address and prefix length to the current standard IPv6 access-list. If a sequence number is specified, the new entry is inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.
Authentication Enhancements						
Authentication Enhancements	Feature	New	Y	Y	Authentication Configuration	The authentication enhancements introduced in this release fall into three areas: improvements to Web-authentication, increased flexibility in the operation of the Guest VLAN, and introduction of the auth-fail VLAN.
Web-authentication Enhancements	Feature	New	Y	Y	Authentication Configuration	These enhancements ensure that the client PC user is presented with the Web-authentication login page as soon as they start web browsing to any address, irrespective of the IP configuration on their PC.
Guest VLAN Enhancements	Feature	New	Y	Y	Authentication Configuration	Guest VLAN enhancements now allow routing from the Guest VLAN to route unauthenticated supplicant's traffic to other VLANs if required, and will relay their DHCP requests to servers in other VLANs if required.
Failed authentication VLAN	Feature	New	Y	Y	Authentication Configuration	The auth-fail VLAN feature allows the Network Administrator to separate the supplicants who attempted authentication, but failed, from the supplicants who did not attempt authentication.
auth auth-fail vlan	Command	New	Y	Y	Authentication Commands	Use this command to enable the auth-fail vlan feature on the specified vlan interface. This feature assigns supplicants (client devices), which have failed port authentication, to the specified vlan interface.

Table 2: New and modified features and commands

Feature/ Command/ MIB	Type	Status	x600	x900/x908	Software Reference Chapter	Description
auth guest-vlan	Command	Modified	Y	Y	Authentication Commands	This command enables and configures the Guest VLAN feature on the interface specified by associating a Guest VLAN with an interface. The new optional routing parameter enables routing from the Guest VLAN to another VLAN, so the switch can lease DHCP addresses and accept access to a limited network.
auth log	Command	New	Y	Y	Authentication Commands	Use this command to configure the types of authentication feature log messages that are output to the log file.
auth-web-server dhcp ip address	Command	New	Y	Y	Authentication Commands	Use this command to assign an IP address and enable the DHCP service on the web authentication server for supplicants (client devices).
auth-web-server dhcp lease	Command	New	Y	Y	Authentication Commands	Use this command to set the DHCP lease time for supplicants (client devices) using the DHCP service on the web authentication server.
auth-web-server mode	Command	New	Y	Y	Authentication Commands	Use this command to configure the mode (from the intercept, none, or promiscuous modes available) on the Web-authentication server for supplicants (client devices).
dot1x max-auth-fail	Command	New	Y	Y	802.1X Commands	Use this command to configure the maximum number of login attempts for a supplicant (client device) using the auth-fail vlan feature, when using 802.1X port authentication on an interface.
Local RADIUS Server						
show radius local-server statistics	Command	Modified	Y	Y	Local RADIUS Server Commands	Use this command to display statistics about the local RADIUS server. Note the 'Unknown username' and 'Invalid passwords' fields in the output have been replaced by a 'Failed Logins' field.
DHCP Snooping						
DHCP Snooping	Feature	New	Y	Y	DHCP Snooping Introduction	DHCP snooping can be used to increase network security and traceability by filtering traffic according to valid DHCP leases. DHCP snooping on the switch supports traffic filtering, DHCP Option 82, ARP security, and MAC address verification.
arp security	Command	New	Y	Y	DHCP Snooping Commands	Use this command to enable ARP security on VLANs.
arp security violation	Command	New	Y	Y	DHCP Snooping Commands	Use this command to specify the action to take if an ARP security violation is detected on the ports.

Table 2: New and modified features and commands

Feature/ Command/ MIB	Type	Status	x600	x900/x908x	Software Reference Chapter	Description
clear arp security statistics	Command	New	Y	Y	DHCP Snooping Commands	Use this command to clear ARP security statistics for the specified ports, or for all ports.
clear ip dhcp snooping binding	Command	New	Y	Y	DHCP Snooping Commands	Use this command to remove dynamic entries from the DHCP snooping database.
clear ip dhcp snooping statistics	Command	New	Y	Y	DHCP Snooping Commands	Use this command to clear DHCP Snooping statistics for the specified ports, or for all ports.
debug arp security	Command	New	Y	Y	DHCP Snooping Commands	Use this command to enable ARP security debugging.
debug ip dhcp snooping	Command	New	Y	Y	DHCP Snooping Commands	Use this command to enable debugging for DHCP snooping.
ip dhcp snooping	Command	New	Y	Y	DHCP Snooping Commands	Use this command to enable DHCP snooping on VLANs.
ip dhcp snooping agent-option	Command	New	Y	Y	DHCP Snooping Commands	Use this command to enable DHCP Option 82 data insertion on the switch.
ip dhcp snooping agent-option allow-untrusted	Command	New	Y	Y	DHCP Snooping Commands	Use this command to enable DHCP Option 82 reception on untrusted ports.
ip dhcp snooping binding	Command	New	Y	Y	DHCP Snooping Commands	Use this command to manually add a dynamic-like entry (with an expiry time) to the DHCP snooping binding database.
ip dhcp snooping database	Command	New	Y	Y	DHCP Snooping Commands	Use this command to set the location of the DHCP snooping database backup file.
ip dhcp snooping delete-by-client	Command	New	Y	Y	DHCP Snooping Commands	Use this command to set the switch to remove a dynamic entry from the DHCP snooping database when it receives a valid DHCP release message for it.
ip dhcp snooping delete-by-linkdown	Command	New	Y	Y	DHCP Snooping Commands	Use this command to set the switch to remove a dynamic entry from the DHCP snooping database when its port goes down.
ip dhcp snooping max-bindings	Command	New	Y	Y	DHCP Snooping Commands	Use this command to set the maximum number of lease entries that can be stored in the DHCP snooping binding database for each of the ports.
ip dhcp snooping subscriber-id	Command	New	Y	Y	DHCP Snooping Commands	Use this command to set a subscriber ID for the ports.
ip dhcp snooping trust	Command	New	Y	Y	DHCP Snooping Commands	Use this command to set the ports to be DHCP snooping trusted ports.

Table 2: New and modified features and commands

Feature/ Command/ MIB	Type	Status	x600	x900/x908	Software Reference Chapter	Description
ip dhcp snooping verify mac-address	Command	New	Y	Y	DHCP Snooping Commands	Use this command to verify that the source MAC address and client hardware address match in DHCP packets on untrusted ports.
ip dhcp snooping violation	Command	New	Y	Y	DHCP Snooping Commands	Use this command to specify the action the switch will take when it detects a DHCP snooping violation on the ports.
ip source binding	Command	New	Y	Y	DHCP Snooping Commands	Use this command to add a static entry to the DHCP snooping database.
service dhcp-snooping	Command	New	Y	Y	DHCP Snooping Commands	Use this command to enable DHCP snooping on the switch.
show arp security	Command	New	Y	Y	DHCP Snooping Commands	Use this command to display ARP security configuration on the switch.
show arp security interface	Command	New	Y	Y	DHCP Snooping Commands	Use this command to display ARP security configuration for ports.
show arp security statistics	Command	New	Y	Y	DHCP Snooping Commands	Use this command to display ARP security statistics.
show debugging arp security	Command	New	Y	Y	DHCP Snooping Commands	Use this command to display the ARP security debugging configuration.
show debugging ip dhcp snooping	Command	New	Y	Y	DHCP Snooping Commands	Use this command to display the DHCP snooping debugging configuration.
show ip dhcp snooping	Command	New	Y	Y	DHCP Snooping Commands	Use this command to display DHCP snooping global configuration on the switch.
show ip dhcp snooping acl	Command	New	Y	Y	DHCP Snooping Commands	Use this command to display information about the access lists using DHCP snooping.
show ip dhcp snooping binding	Command	New	Y	Y	DHCP Snooping Commands	Use this command to display all dynamic and static entries in the DHCP snooping binding database.
show ip dhcp snooping interface	Command	New	Y	Y	DHCP Snooping Commands	Use this command to display information about DHCP snooping configuration and leases for specified ports, or all ports.
show ip dhcp snooping statistics	Command	New	Y	Y	DHCP Snooping Commands	Use this command to display DHCP snooping statistics.
show ip source binding	Command	New	Y	Y	DHCP Snooping Commands	Use this command to display static entries in the DHCP snooping database.

Table 2: New and modified features and commands

Feature/ Command/ MIB	Type	Status	x600	x600/806x	Software Reference Chapter	Description
DHCP						
clear ip dhcp binding	Command	New	Y	Y	Dynamic Host Configuration Protocol (DHCP) Commands	On dynamically allocated bindings this command clears either a specific lease binding, or the lease bindings specified by the command.
SNMP						
snmp-server enable trap	Command	Modified	Y	Y	SNMP Commands	This command can now enable the switch to send DHCP snooping notifications (traps).
SNMP MIB						
AT-DHCPSN-MIB	MIB	New	Y	Y	SNMP MIBs	This MIB contains objects for displaying and managing DHCP snooping and ARP security information on the switch.
Private MIBs	MIB	New	Y	Y	SNMP MIBs	Support for the sFlow Agent MIB has been added.
Trigger Enhancements						
type stack disabled-master	Command	New	Y	Y	Trigger Commands	This command (configured to the stack) selects a pre-configured trigger that will activate on a stack member if it becomes the disabled master.
sFlow						
sFlow Introduction	Feature	New	Y	Y	sFlow Introduction	sFlow®1 provides the ability to monitor traffic in data networks containing switches and routers. This feature adds the sFlow Agent capability.
debug sflow	Command	New	Y	Y	sFlow Commands	This command enables sFlow® debug message logging, for sFlow sampling and polling activity on the specified ports. If no ports are specified, sampling and/or polling debug messages are enabled for all ports.
debug sflow agent	Command	New	Y	Y	sFlow Commands	This command enables sFlow® debug message logging that is not specific to particular ports. For example, sending an sFlow datagram to the collector.
sflow agent (address)	Command	New	Y	Y	sFlow Commands	This command sets the sFlow® agent IP address on the switch. This address is inserted into every sFlow datagram sent from the sFlow agent switch, to the sFlow collector device. The sFlow collector then use this address for SNMP to uniquely identify and access the switch.
sflow collector (address)	Command	New	Y	Y	sFlow Commands	This command sets the sFlow® agent's collector IP address and/or UDP port. This is the destination IP address and UDP port, for sFlow datagrams sent from the sFlow agent. The IP address can be any valid IPv4 or IPv6 address.
sflow collector max-datagram-size	Command	New	Y	Y	sFlow Commands	This command sets the maximum size of the sFlow® datagrams sent to the collector.

Table 2: New and modified features and commands

Feature/ Command/ MIB	Type	Status	x600	x900/x908	Software Reference Chapter	Description
sflow enable	Command	New	Y	Y	sFlow Commands	This command enables sFlow® globally on the switch. Note that sFlow cannot be enabled if Tx port mirroring is enabled on any port on the device.
sflow max-header-size	Command	New	Y	Y	sFlow Commands	This command sets the maximum header size of the ethernet frames sampled on a specified port. The maximum header size is measured in bytes, referenced from the first byte of the ethernet destination address and excludes the ethernet FCS fields.
sflow polling-interval	Command	New	Y	Y	sFlow Commands	This command sets the sFlow® counter polling interval (in seconds) for the specified ports. A value of 0 disables polling. A counter sample is taken every N seconds where N is the value set by this command.
sflow sampling-rate	Command	New	Y	Y	sFlow Commands	This command sets the mean sFlow® sampling rate for the specified ports. Sampling occurs every N frames (on average), where N is the rate value set via this command. The sampling rate applies to ingress and egress frames independently.
show debugging sflow	Command	New	Y	Y	sFlow Commands	This command displays sFlow® debug settings for agent operation, and for sampling and polling on specific interface ports. If no interface ports are specified, sampling and polling will be applied to all ports.
show running-config sflow	Command	New	Y	Y	sFlow Commands	This command displays the running system information specific to the sFlow feature.
show sflow	Command	New	Y	Y	sFlow Commands	This command displays non-port-specific sFlow agent configuration and operational status.
show sflow interface	Command	New	Y	Y	sFlow Commands	This command displays sFlow agent sampling and polling configuration for specified ports.
undebug sflow	Command	New	Y	Y	sFlow Commands	This command applies the functionality of the no debug sflow command.
VCStack						
reboot rolling	Command	New	Y	Y	Stacking Commands	This command allows a stack to be rebooted in a rolling sequence to minimize downtime. The stack master is rebooted causing the remaining stack members to failover and elect a new master.
reload rolling	Command	New	Y	Y	Stacking Commands	This command performs the same function as the reboot rolling command.
remote-login	Command	New	Y	Y	Stacking Commands	This command is used only on the master in order to log onto the CLI of another stack member. In most respects this the result is as if being logged into the stack master. Config commands are still broadcast to all stack members, but show commands, and commands that access the file system are executed locally.

Table 2: New and modified features and commands

Feature/ Command/ MIB	Type	Status	x600	x900/x908	Software Reference Chapter	Description
show provisioning (stack-member)	Command	New	Y	Y	Stacking Commands	This command shows the provisioning status of all installed or provisioned hardware.
show stack	Command	Modified	Y	Y	Stacking Commands	This command now shows provisioning details.
stack fallback-config (Disabled)	Command	Modified	Y	Y	Stacking Commands	This command has been disabled. To simplify stack recovery, stub reconfiguration is now achieved by using a trigger that is generated by the type stack disabled-master command on page 87.23.
switch provision	Command	New	Y	Y	Stacking Commands	This command enables you provide the configuration for a new VCStack member switch prior to physically connecting it to the stack. To run this command, the stack position must be vacant. The selected hardware type must be compatible existing stack hardware.
GUI						
Switching > Power over Ethernet	GUI tab	New	Y	Y	Appendix C: GUI Reference	The Switching > Power over Ethernet menu tab allows you to monitor and configure PoE on your PoE switch. You can monitor PoE status, and configure PoE ports and the PSE power.

Installing this Software Version

To use this software version, your switch must already be running AlliedWare Plus. Contact your distributor or reseller for more information.

To install and enable this software version, use the following steps:

1. Copy the software version file (.rel) onto your TFTP server.

2. If necessary, delete or move files to create space in the switch's Flash memory for the new file.

   To see the memory usage, use the command:

   ```
   awplus#show file systems
   ```

   To list files, use the command:

   ```
   awplus#dir
   ```

   To delete files, use the command:

   ```
   awplus#del <filename>
   ```

   You cannot delete the current boot file.

3. Copy the new release from your TFTP server onto the switch.

   ```
   awplus#copy tftp flash
   ```

   Follow the onscreen prompts to specify the server and file.

4. Set the switch to reboot with the new software version either for x600 series switches:

   ```
   awplus#configure terminal
   awplus(config)#boot system r6-5.3.4-0.1.rel
   ```

   or for x908 / x900 series switches:

   ```
   awplus#configure terminal
   awplus(config)#boot system r1-5.3.4-0.1.rel
   ```

   Return to Privileged Exec mode and check the boot settings, by using the commands:

   ```
   awplus(config)#exit
   awplus#show boot
   ```

5. Reboot using the new software version.

   ```
   awplus#reload
   ```

Installing the GUI

This section describes how to install and set up the AlliedWare Plus GUI using an SD card or a TFTP server. The version number in the GUI Java applet filename (.jar) gives the earliest version of the software file (.rel) that the GUI can operate with.

To install and run the AlliedWare Plus GUI requires the following system products and setup:

- PC Platform:
  Windows XP SP2 and up / Windows Vista SP1 and up
- Browser: (must support Java Runtime Environment (JRE) version 6)
  Microsoft Internet Explorer 7.0 and up / Mozilla Firefox 2.0 and up

To install the GUI on your switch, use the following steps:

1. Copy to the GUI Java applet file (**.jar** extension) onto your TFTP server or SD card.

2. Connect to the switch's management port, then log into the switch.

3. If necessary, delete or move files to create space in the switch's Flash memory for the new file.

   To see the memory usage, use the command:

   ```
   awplus#show file systems
   ```

   To list files, use the command:

   ```
   awplus#dir
   ```

   To delete files, use the command:

   ```
   awplus#del <filename>
   ```

   You cannot delete the current boot file.

4. Assign an IP address for connecting to the GUI. Use the commands:

   ```
   awplus#configure terminal
   awplus(config)#interface vlan1
   awplus(config-if)#ip address <address>/<prefix-length>
   ```

   Where <*address*> is the IP address that you will subsequently browse to when you connect to the GUI Java applet. For example, to give the switch an IP address of 192.168.2.6, with a subnet mask of 255.255.255.0, use the command:

   ```
   awplus(config-if)#ip address 192.168.2.6/24
   ```

5. If required, configure a default gateway for the switch.

   ```
   awplus(config-if)#exit
   awplus(config)#ip route 0.0.0.0/0 <gateway-address>
   ```

   Where <*gateway-address*> is the IP address for your gateway device. You do not need to define a default gateway if you browse to the switch from within its own subnet.

6. Copy the GUI file onto your switch from the TFTP server or SD card.

   TFTP server: Use the command:

   ```
   awplus#copy tftp://<server-address>/<filename.jar> flash:/
   ```

   where <*server-address*> is the IP address of the TFTP server, and where <*filename.jar*> is the filename of the GUI Java applet.

   SD card: Insert the SD card into the SD slot on the front of your switch, and use the command:

   ```
   awplus#copy card:/<filename.jar> flash:/
   ```

   where <*filename.jar*> is the filename of the GUI Java applet.

7. Create a user account for logging into the GUI.

   ```
   awplus(config)#username <username> privilege 15 guiuser password
                  <password>
   ```

   You can create multiple users to log into the GUI. For information about the username command, see the AlliedWare Plus Software Reference.

8. Log into the GUI.

   Start a browser and enter the switch's IP address. The GUI starts up and displays a login screen. Log in with the username and password specified in the previous step.

Errata to the Software Reference

The following update is a correction to the *Software Reference for AlliedWare Plus 5.3.4-0.1*

Note that the show cli and show list commands shown in the *Software Reference for AlliedWare Plus 5.3.4-0.1* are not supported in this release.

Note that the icmp-redirect command will operate on the x600 series only. The ip redirects command in the *Software Reference for AlliedWare Plus 5.3.4-0.1* is not supported in this release.

icmp-redirect (x600)

This command re-enables ICMP redirects globally. Note that ICMP redirects are enabled by default. Use this command to allow the sending of ICMP redirects whenever the switch receives a packet that is routed on the same interface that the packet was sent on.

Use the no variant of this command to disallow the sending of ICMP redirects whenever the switch receives a packet that is routed on the same interface that the packet was sent on. Use the no variant of this command to disable the sending of ICMP redirects globally.

Syntax

```
icmp-redirect
no icmp-redirect
```

Mode Global Configuration

Default ICMP redirects are enabled by default.

Usage ICMP redirect messages are used to notify hosts that a better route is available to a destination. ICMP redirects are used when a packet is routed into the switch on the same interface that the packet is routed out of the switch. ICMP redirects are also used when the subnet or network of the source address is on the same subnet or network as the next-hop address for a packet.

This command enables and disables the copying, and therefore CPU processing, of IPv4 and IPv6 packets being L3 switched coming in and going out the same interface. So when the switch receives IP packets to forward on the same interface that the packets came from, such as when traffic goes in and out of a multihomed interface, then the packets will cause the CPU utilization to be higher than normal. The CPU utilization is increased by the CPU inspecting packets for ICMP redirection. Turn off the ICMP redirection feature to avoid an increase in CPU utilization.

Examples To re-enable ICMP redirects on the switch, which will enable the CPU inspection of packets coming in and going out of the same interface, use the following commands:

```
awplus# configure terminal
awplus(config)# icmp-redirect
```

To disable ICMP redirects on the switch, which will disable the CPU inspection of packets coming in and going out of the same interface, use the following commands:

```
awplus# configure terminal
awplus(config)# no icmp-redirect
```

Related Commands show running-config

sflow agent (address)

This command sets the sFlow® agent IP address on the switch. This address is inserted into every sFlow datagram sent from the sFlow agent switch to the sFlow collector device. The sFlow collector can then uses this address to uniquely identify and to access the switch, such as for SNMP. We therefore recommend that you change this address as little as possible.

Although the agent address can be set to any valid IPv4 or IPv6 address; we recommended that you set the sFlow® agent IP address to be the local address[1] that is configured on the switch. This ensures that the sFlow collector can maintain connectivity to the switch irrespective of the addition or deletion of VLAN interfaces (each of which will have its own specific IP address). Note that sFlow is rendered inactive whenever the agent address is not set.

1. For information on local addresses and how to set them up, see the interface (to configure) command on page 12.3.

The no variant of this command applies its default setting.

Syntax

```
sflow agent {ip <ip-address>|ipv6 <ipv6-address>}
no sflow agent {ip <ip-address>|ipv6 <ipv6-address>}
```

Parameter	Description
<ip-address>	The IPv4 address of the switch that is acting as the sFlow agent.
<ipv6-address>	The IPv6 address of the switch that is acting as the sFlow agent. The IPv6 address uses the format X:X::X:X.

Default The sFlow agent address is unset.

Mode Global Configuration

Examples To set the sFlow agent (IPv4) address to `192.0.2.23`, use the command:

```
awplus# configure terminal
awplus(config)# sflow agent ip 192.0.2.23
```

To set the sFlow agent (IPv6) address to `2001:0db8::1`, use the command:

```
awplus# configure terminal
awplus(config)# sflow agent ipv6 2001:0db8::1
```

Related Commands show running-config sflow
show sflow

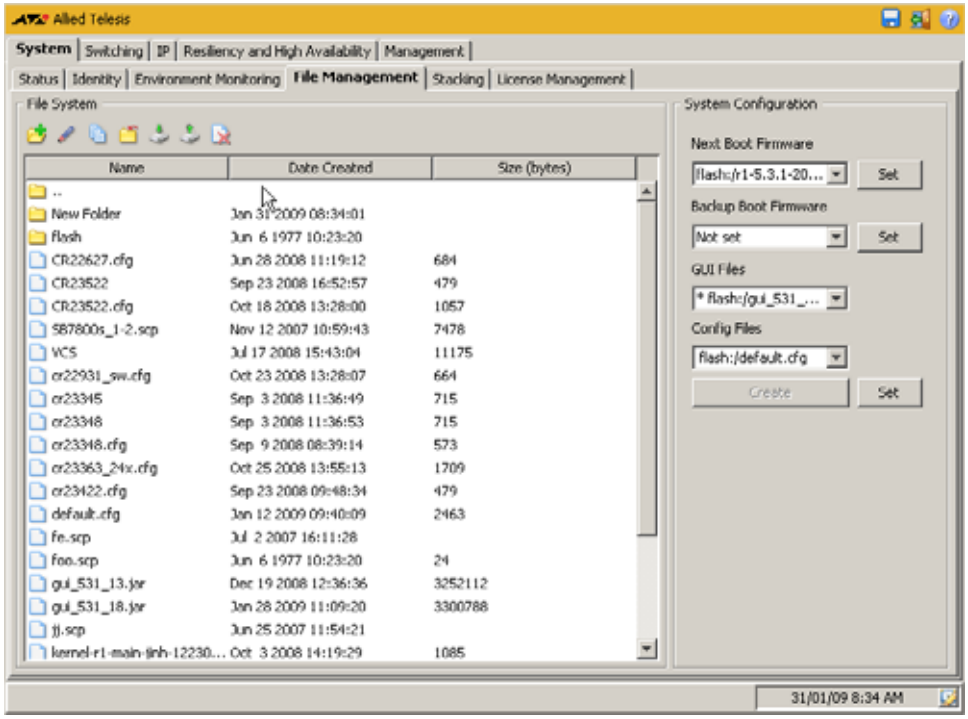
GUI Errata

System > File Management

The System > File Management menu tab allows you to create, copy, delete, upload or download files to and from the switch.

Menu Tab

Figure 1-3: Example showing the **System > File Management** menu tab:



Description: File System

Label / Field / Button	Description
`File System`	Displays file names, file dates, and file sizes of files in Flash, NVS or SD-card.
`File System / Add Folder`	Select the folder you want to create a new sub-folder in then click on the Add Folder icon located directly below the File System label.
`File System / Rename File or Folder`	Select the file or folder you want to rename then click on the Rename File or Folder icon located directly below the File System label.
`File System / Copy File or Folder`	Select the file or folder you want to rename then click on the Copy File or Folder icon located directly below the File System label.Choose the Destination Folder from the drop down list in the Copy File dialog then select OK to copy the file or folder to the chosen destination.

Label / Field / Button	Description (cont.)
File System / Move File or Folder	Select the file or folder you want to move then click on the Move File or Folder icon located directly below the File System label. Choose the Destination Folder from the drop down list in the Move File dialog then select OK to move the file or folder to the chosen destination.
File System / Download File	Select the file you want to download then click on the Download File icon located directly below the File System label.
File System / Upload File	Select the file you want to upload then click on the Upload File icon located directly below the File System label.
File System / Delete File or Folder	Select the file or folder you want to delete then click on the Delete File or Folder icon located directly below the File System label.

Description: System Configuration

Label / Field / Button	Description
System Configuration	Configures running and backup software, GUI software, and configuration files in Flash or card memory available on the switch.
System Configuration / Next Boot Firmware	Choose the Next Boot Firmware .rel file and path from the drop down list then click Set to make this file the firmware that starts after reboot.
System Configuration / Backup Boot Firmware	Choose the Backup Boot Firmware .rel file and path from the drop down list then click Set to make this file the fallback boot firmware at reboot.
System Configuration / GUI Files	Displays the GUI file name and file location on the switch and indicates the currently running GUI file with a prefixed asterisk (*) (e.g. `* flash:/gui_534_06.jar`). Note that you cannot set the GUI version from within the GUI itself. See the GUI installation instructions in *Appendix C: GUI Reference* of the current *AW+ Software Reference* to install GUI files.
System Configuration / GUI Files	Choose the GUI Files .jar file and path from the drop down list then click Set to make this file the GUI file that you connect to after reboot.
System Configuration / Config Files	Choose the Config Files .cfg file and path from the drop down list then click Set to make this file the config file that the switch uses at reboot.

System > Status

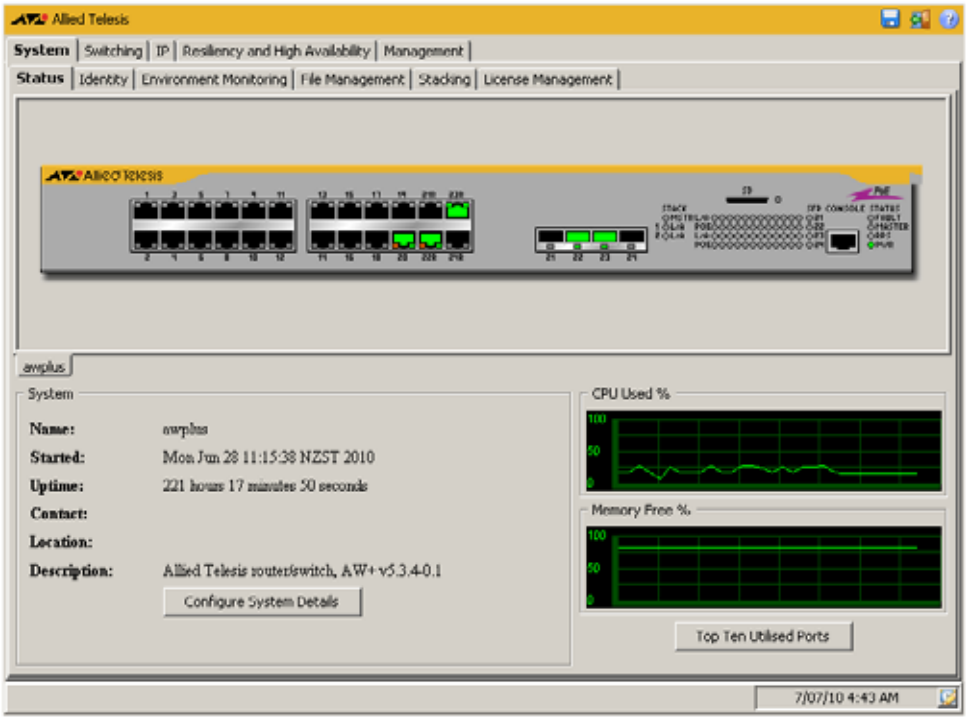
The System > Status menu tab enables you to display and configure basic system information.

The CPU Used % and Memory Free % graphs provide a brief history of CPU and memory usage.

Note For systems equipped and configured using VCStack, there is a separate tab for each stack member with the system name displayed on each tab.

Menu Tab

Figure 1-4: Example showing the **System > Status** menu tab:



Description

Display Label / Field	Description
System / Name	Specifies the network name of the system, as set with the 'hostname' command in the CLI.
System / Started	Date and time the switch was last booted.
System / Uptime	Elapsed time since the last boot.
System/ Contact	Contact details for system maintenance.
System/ Location	Location of the switch

Display Label / Field	Description (cont.)
System / Description	Description of the switch, including manufacturer, model, and software version.
Top Ten Utilised Ports	Displays a sorted list of the ten most used ports listed by port and its utilization. You can rearrange and resort the list by port or utilization.

Description

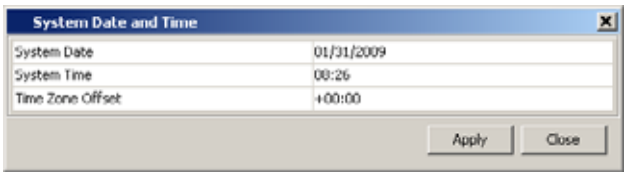
Configuration Button / Field	Description
System Time & Date (icon)	Add or modify System Date, System Time, UTC Time Zone Offset.
Configure System Details	Add or modify System Name, System Contact, System Location.
Configure System Details / System Name	Configures the network name of the system.
Configure System Details / System Contact	Configures the contact information for the system, from 0 to 255 characters long. Valid characters are any printable characters and spaces.
Configure System Details / System Location	Configures the location of the system, from 0 to 255 characters long. Valid characters are any printable characters and spaces.

System > Status > System Date and Time

The System > Status > System Date and Time dialog allows you to configure the date and time for the switch.

Configuration Dialog

Figure 1-5: Example showing **System > Status > System Date and Time** dialog:



Description

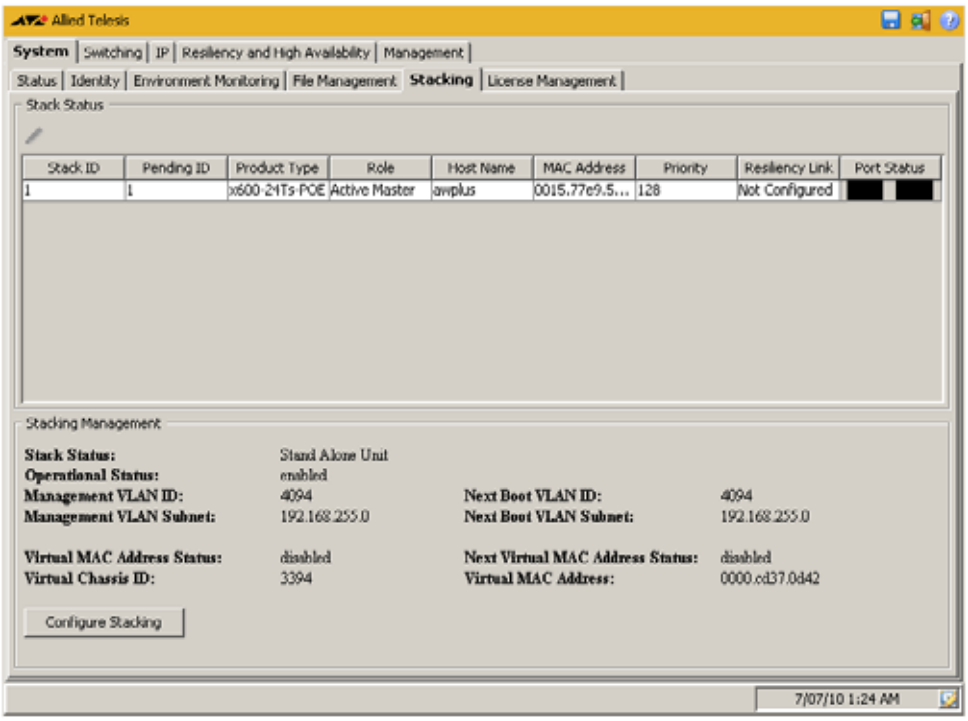
Label / Field / Button	Description
System Date	Enter the current system date in month, day, and year format.
System Time	Enter the local time for the system clock in hours and minutes.
Time Zone Offset	Enter the offset to the UTC (Coordinated Universal Timezone) for a local timezone in hours and minutes.

System > Stacking

The System > Stacking menu tab allows you to display and monitor a summary of the identity and status of stack members, plus you can also configure the VLAN ID and IP subnets used for internal VCStack communication.

Menu Tab

Figure 1-6: Example showing the **System > Stacking menu tab**:



Description: Stacking Management

Label / Field / Button	Description
`Stacking Management / Stack Status`	The stack's overall status. Note that a warning is issued if the stack is not connected in a standard ring topology.
`Stacking Management / Operational Status`	The status of the stack - either enabled or disabled.
`Stacking Management / Management VLAN ID`	The VLAN ID currently used for stack management. The default stack management VLAN ID is 4094.
`Stacking Management / Next Boot VLAN ID`	The VCS management VLAN ID to be assigned after the next reboot.
`Stacking Management / Management VLAN Subnet`	The VLAN subnet currently used for stack management.
`Stacking Management / Next Boot VLAN Subnet`	The stacking management VLAN subnet address after rebooting.

Label / Field / Button	Description (cont.)
Stacking Management / Virtual MAC Address Status	Indicates whether the virtual MAC address is enabled or disabled.
Stacking Management / Next Virtual MAC Address Status	Indicates whether the next virtual MAC address is enabled or disabled.
Stacking Management / Virtual Chassis ID	Displays the current virtual chassis ID.
Stacking Management / Virtual MAC Address	Displays the virtual MAC address used by the stack.
Configure Stacking	Configures the VCS management VLAN ID and the subnet address of the VCS management VLAN.

Description: Stack Status

Label / Field / Button	Description
Stack Status / Stack ID	The Stack member ID.
Stack Status / Pending ID	The Stack member ID to be assigned to the device after the next reboot.
Stack Status / Product Type	The Stack member product type; for example, SwitchBlade x908.
Stack Status / Role	Stack member's role in the stack (either master or backup).
Stack Status / Host Name	The host name of the Stack member.
Stack Status / MAC Address	Stack member's hardware MAC address. Note that frames from devices within a stacked virtual chassis will carry the source address of the stack master.
Stack Status / Priority	The priority for election of stack master (0 to 255). The lowest number has the highest priority. Note that where stack members have the same priority setting, the switch with the lowest MAC address will become the stack master.
Stack Status / Resiliency Link	Status of the stack members resiliency link. Can be one of: configured (1), successful (2), failed (3), notConfigured (4).
Stack Status / Port Status	The status of the stack port, can be: "Down", "Neighbour incompatible", "Discovering neighbour", or "Learnt neighbour <*neighbour member ID*>".